PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06

A1

(11) International Publication Number: **WO 00/27089**

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25215

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:
60/106,290 30 October 1998 (30.10.98) US

(71) Applicant: LOCKSTAR, INC. [US/US]; 777 Passaic Avenue, Clifton, NJ 07012 (US).

(72) Inventors: ORRIN, Steven, M.; 43 Conforti Avenue #77, West Orange, NJ 07052 (US). RUSSELL, James, P.; 27 Freeman Place, Nutley, NJ 07110 (US). GOLDBERG, Brian, D.; 1434 Pleasant Valley Way, West Orange, NJ 07052 (US). OLIK, Zbigniew, T.; 103 Lexington Avenue, Rochelle Park, NJ 07662 (US). OVITS, Mordechai; 113 Parkville Avenue, Brooklyn, NY 11230 (US). BENENSON, Paul; Apartment 3B, 127 Garden Street, Hoboken, NJ 07030 (US). MARCELLUS, Daniel, H.; 27 Cross Ridge Road, Tuxedo, NY 10987 (US).

(74) Agent: MILLER, Joel; 17 Westwood Drive South, West Orange, NJ 07052–1822 (US).

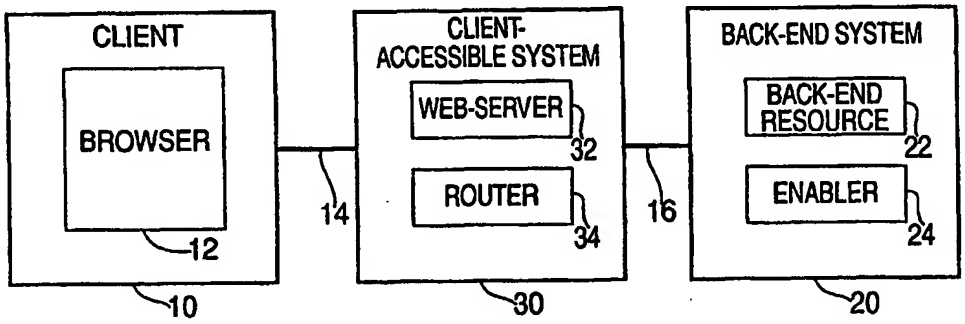
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE AUTHENTICATION FOR ACCESS TO BACK–END RESOURCES



(57) Abstract

By establishing a secure channel from a client to a back–end resource after the client is authenticated, both security and authentication can be achieved. Before access is permitted, two levels of authentication are provided by first seeking a client–side certificate and then having the client subsequently decrypt an encrypted message. Authorization for access to a back–end resource can be controlled by requiring a transaction–specific authorization device provided to the client in the encrypted message.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURE AUTHENTICATION FOR ACCESS TO BACK-END RESOURCES

Technical Field and Background Art

This application claims the benefit of U.S. Provisional Application no. 60/106,290, filed October 30, 1998.

Traditionally, access to back-end resources, such as corporate databases, has been accomplished within secure mainframe environments or other internal networks. In such settings, security and user authentication are achieved with a high degree of reliability.

With the advent of the Internet, remote users need to access such resources from outside the protected environment. However, when these resources are accessed over the Internet, additional measures are required to provide assurances of security and user authentication.

Brief Description of the Drawings

Figure 1 is a block diagram of a system providing security and authentication;

Figure 2 is a flow chart of the operation of the system of Figure 1.

Modes for Carrying Out the Invention

Data security and user authentication can be achieved in an Internet environment by establishing a secure channel from the user or client to the back-end resource and then by providing an authorization device which the user in turn employs to access the back-end resource.

In one configuration, illustrated in the block diagram of Figure 1, a client 10, using an Internet browser 12 equipped with the means necessary

to create a secure session, accesses a back-end system 20 on which a back-end resource 22 resides, through a client-accessible system 30. The back-end resource 22 may be a database or some other source of data or device that the client wishes to access.

The interconnection 14 between the client 10 and the client-accessible system 30 can be over a network such as the Internet or through some other medium. Similarly, the link 16 between the client-accessible system 30 and the back-end system 20 can be over a network such as the Internet or through some other data link.

The process has two parts: first, a secure connection is established and the client is authenticated and, second, the client accesses the desired information. A secure connection from the client 10 to the back-end system 20 can be created using a secure protocol such as SSL (secure socket layer). Software resident on the client-accessible system 30, designated a router 34, and on the back-end system 20, designated an enabler 24, allows the establishment of the secure session from the client 10 to the back-end system 20 using well-known techniques for the purpose of authenticating the client 10. In the case of SSL, a public key certificate, attesting to and establishing the identity of the client 10, is requested from the client by the enabler 24. The public key certificate is then used by the back-end system 20 to create the secure session. As is customary in SSL, the enabler 24 also provides a certificate to the client 10.

The process begins with a query from the client 10. To acquire a specific piece of information from the back-end resource 22, the client 10 enters a pre-determined URL on its Internet browser 12 specifying a port on the client-accessible system 30 linked to the router 34. The URL may assume the following form:

https://hostname:7777/abc.cgi

The "https" designation within the above URL indicates that a secure session -- in this example, SSL -- is to be established between the browser 12 and the client-accessible system 30. Since the URL specifies "hostname:7777," the browser 12 will create a secure session at port 7777 of the destination known as "hostname." That port indicates the location of the router 34, which passes the query to the enabler 24.

Once a secure session is created between the client 10 and the back-end system 20, the browser 12 sends along the rest of the URL (e.g., "abc.cgi"), the actual request, through the router 34 in encrypted form. Note that all information exchanged from hereon out is encrypted. The request, "abc.cgi," is the name of the routine that will retrieve the information from the back-end resource 22. The router 34 passes this encrypted message to the enabler 24 on the back-end system 20. The enabler 24 decrypts the request and determines whether the request will be authorized and access permitted.

Assuming that the client 10 is authorized entry, the enabler 24 will send a message back to the client 10 over the secure connection. The message can contain a redirection command such as a new or redirect URL, sending the client 10 to a different port on the client-accessible system 30, or to an entirely different client-accessible system, through which the desired information will be provided. The redirect URL may be of the form:

https://hostname/abc.cgi?{W}

Again, abc.cgi is the routine for retrieving the information. The redirect URL may also contains an authorization device, designated W in the URL above. One such authorization device can be a web ticket. This authorization device or web ticket is the permission from the back-end resource 22

allowing the web-server 32 to act on behalf of the client for the purpose of accessing the requested information.

When the client 10 receives the messages with the authorization device or web ticket, it arrives of course in encrypted form. By virtue of the act of decrypting the message (in SSL, using the originally-created session key), the client 10 has further authenticated itself. Thus, the process described here offers dual authentication, once upon creating the secure session and again when the client 10 decrypts the redirect message.

The client 10 then goes to the new or redirect URL, entering a presentation server such as a a web-server 32 on the original client-accessible system 30 through a different port (e.g., port 443 -- the default secure port) or perhaps another web-server residing on a different system. For purposes of this discussion, the presentation server will be referred to as a "web-server" hereafter, but it should be understood that the depicted web-server may be any suitable device.

The redirect URL also contains an "https" designation, indicating that a secure session is to be created between the web-server 32 and the client 10. The authorization device or web ticket is forwarded to the back-end system 20 and, if the authorization device is deemed to be valid, the request is honored. The requested information is then passed from the back-end resource 22 to the web-server 32, which generates a web page containing the information. This page is then sent to the client 10 via the secure connection.

The web ticket may include a time stamp to limit the time of its validity. Alternatively, the authorizing elements of the web ticket can be changed after a period of time, effectively invalidating the web ticket at the time of the change, or it may be usable only once.

The foregoing method can be used with multiple back-end resources and/or client-accessible systems. For example, the client accessible system could have multiple routers. Further, the method can be used in a system with multiple layers of client-accessible systems, i.e., web-servers, application servers, and the like. Where there are multiple layers, the method is repeated in "nested" fashion, repeating the process of establishing a secure session, exchanging certificates, and providing a redirect with an authorization device at each layer until the last layer, a back-end resource, is reached.

In the foregoing examples, SSL is used to create a secure session. Other schemes could be employed to achieve the same purpose.

What is claimed is:

1. A method for permitting a client to access a back-end resource via network-based client-accessible systems comprising web-servers, comprising the steps of:

establishing a first secure connection between the client and the back-end system via a client-accessible system, the step of establishing a first secure connection comprising the step of obtaining client authentication;

initiating a request by the client for information from the back-end resource;

generating an authorization device and redirection command;

passing the authorization device and the redirection command to the client;

establishing a second secure connection between the client and a web-server according to the redirection command;

presenting the authorization device to the back-end system;

passing the information from the back-end resource to the web-server; and

passing the information from the web-server to the client via the second secure connection.

2. A method as set forth in claim 1, where the step of obtaining client authentication comprises the steps of providing a client certificate to the back-end resource and using the client certificate to create the secure session.

3. A method as set forth in claim 1, further comprising the step of encrypting the authorization device and redirection command prior to the

step of passing the authorization device and redirection command to the client.

4. A method for establishing a secure connection between a client and a back-end system via network-based client-accessible systems comprising web-servers, comprising the steps of:

establishing a first secure connection between the client and the back-end system via a client-accessible system, the step of establishing a first secure connection comprising the step of obtaining client authentication;

initiating a request by the client for information from the back-end resource;

generating an authorization device and redirection command;

passing the authorization device and the redirection command to the client;

establishing a second secure connection between the client and a web-server according to the redirection command; and

presenting the authorization device to the back-end system.

5. A method as set forth in claim 4, where the step of obtaining client authentication comprises the steps of providing a client certificate to the back-end resource and using the client certificate to create the secure session.

6. A method for authorizing remote client access to a back-end resource via a web-server on a network, comprising the steps of:

generating an authorization device;

passing the authorization device to the client through a first secure connection;

establishing a second secure connection between the client and a web-server;

passing the authorization device to the web-server via the second secure connection;

passing the authorization device from the web-server to the back-end resource;

passing the information from the back-end resource to the web-server; and

passing the information from the web-server to the client via the second secure connection.

7. A method as set forth in claim 6, further comprising the step of encrypting the authorization device and redirection command prior to the step of passing the authorization device and redirection command to the client.

8. A system for establishing a secure connection between a client and a back-end resource; comprising:

a back-end system comprising

the back-end resource; and

an enabler, the enabler comprising

means for authenticating the client; and

means for authorizing retrieval of information for the client; and

at least one network-based client-accessible system comprising

at least one web-server; and

a router comprising means for communicating with the client and the enabler.

9. A system as set forth in claim 8, where the means for authenticating the client comprises means for receiving a certificate of authentication from the client via the router.

10. A system as set forth in claim 8, where the means for authorizing retrieval comprises means for generating an authorizing device for receipt by the client via the router and subsequent presentation to the back-end system.

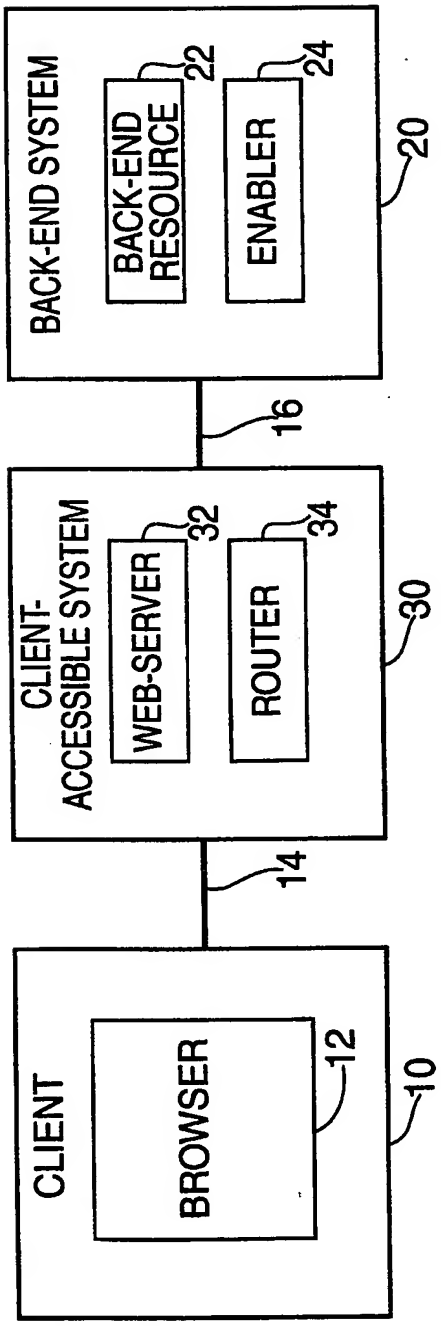

BACK-END SYSTEM
BACK-END RESOURCE
22
ENABLER
24
20
16
CLIENT-ACCESSIBLE SYSTEM
WEB-SERVER
32
ROUTER
34
30
14
CLIENT
BROWSER
12
10

FIG. 1

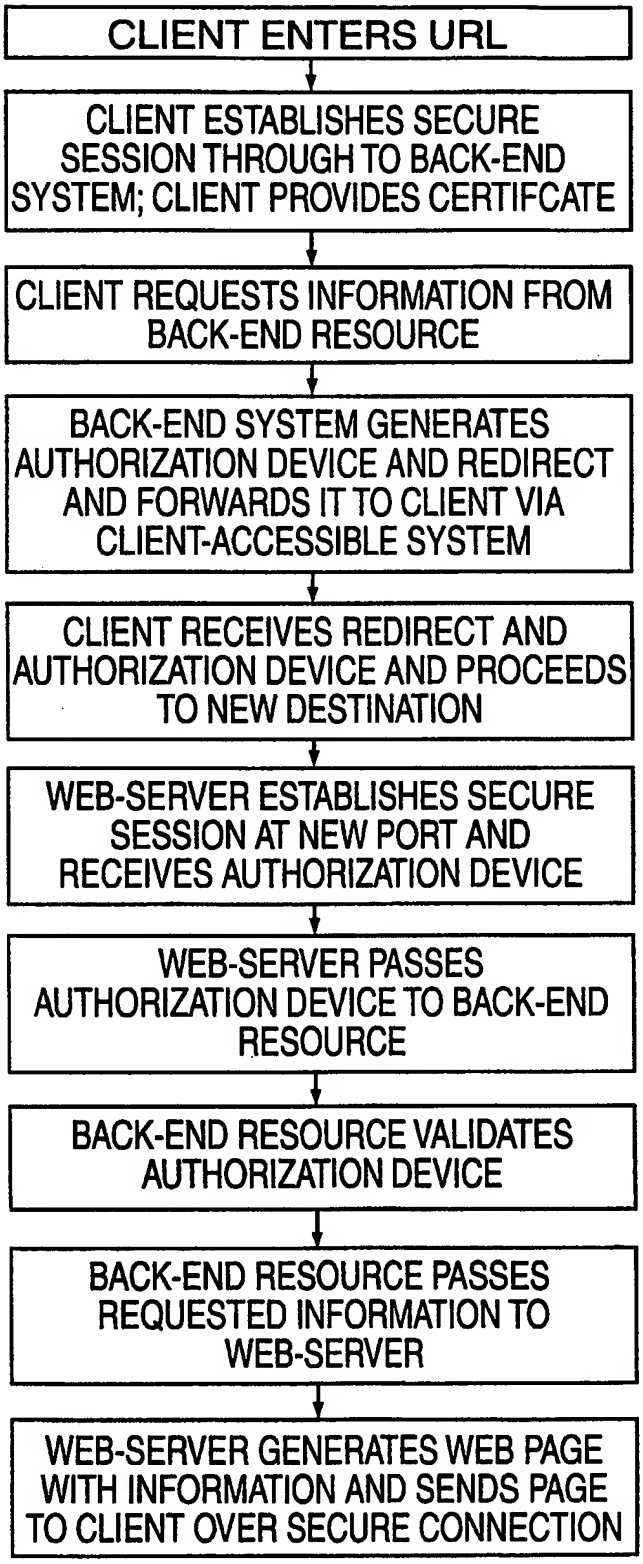

CLIENT ENTERS URL
CLIENT ESTABLISHES SECURE SESSION THROUGH TO BACK-END SYSTEM; CLIENT PROVIDES CERTIFCATE
CLIENT REQUESTS INFORMATION FROM BACK-END RESOURCE
BACK-END SYSTEM GENERATES AUTHORIZATION DEVICE AND REDIRECT AND FORWARDS IT TO CLIENT VIA CLIENT-ACCESSIBLE SYSTEM
CLIENT RECEIVES REDIRECT AND AUTHORIZATION DEVICE AND PROCEEDS TO NEW DESTINATION
WEB-SERVER ESTABLISHES SECURE SESSION AT NEW PORT AND RECEIVES AUTHORIZATION DEVICE
WEB-SERVER PASSES AUTHORIZATION DEVICE TO BACK-END RESOURCE
BACK-END RESOURCE VALIDATES AUTHORIZATION DEVICE
BACK-END RESOURCE PASSES REQUESTED INFORMATION TO WEB-SERVER
WEB-SERVER GENERATES WEB PAGE WITH INFORMATION AND SENDS PAGE TO CLIENT OVER SECURE CONNECTION

FIG. 2

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/US 99/25215

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 805 803 A (ABADI MARTIN ET AL) 8 September 1998 (1998-09-08) column 2, line 21-60 column 3, line 6 -column 5, line 46 figures 1-3	1-10
X	WO 98 36522 A (GTE LABORATORIES INC) 20 August 1998 (1998-08-20)	1,3,6-8
A	page 8, line 7-26 page 10, line 4 -page 16, line 2	2,4,5,9, 10
A	WO 98 40809 A (CHA TECH SERV INC) 17 September 1998 (1998-09-17) page 2, line 12 -page 3, line 30 page 7, line 2 -page 9, line 2 claim 1	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 April 2000	20/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lázaro Lõpez, M.L.

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inten. nal Application No
PCT/US 99/25215

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5805803 A	08-09-1998	NONE	
WO 9836522 A	20-08-1998	US 5923756 A	13-07-1999
		EP 0960500 A	01-12-1999
WO 9840809 A	17-09-1998	US 5903721 A	11-05-1999
		AU 6549498 A	29-09-1998
		NO 994428 A	09-11-1999